Министерство образования Республики Беларусь

Учреждение образования

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Факультет инфокоммуникаций

Кафедра защиты информации

Практическая работа № 4

«Уязвимости виртуальных локальные сетей»

Шифр: 173

Проверила:

Белоусова Е.С.

Выполнила:

ст. гр. 961401

Савченко Е.А.

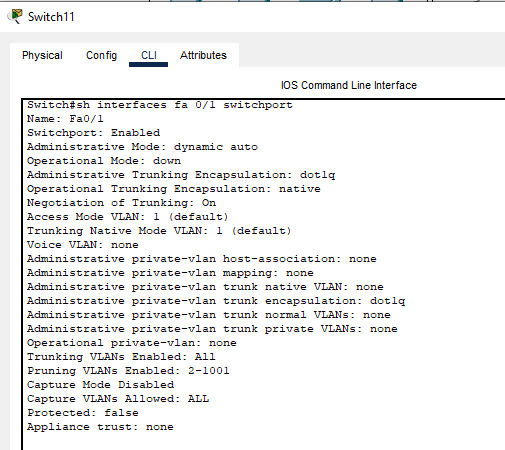
­

Минск 2022

**Цель:** проанализировать уязвимости VLAN и принципы реализации атак, эксплуатирующие данные уязвимости. Научиться реализовывать защиту от атак на виртуальные локальные сети.

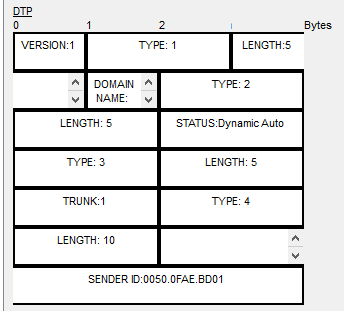
**Ход работы:**

2. Происходит атака на порт fa 0/1 Switch 11, где не настроены режимы trunk/acsecc и можно увидеть, что статус порта dynamic auto.

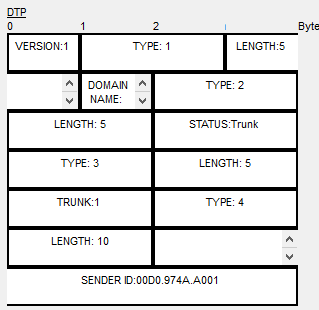


Тогда злоумышленник устанавливает на своем switch 10 attacker порт fa 0/1 в режиме trunk, что приведет в автоматическом режиме к согласованию в trunk.

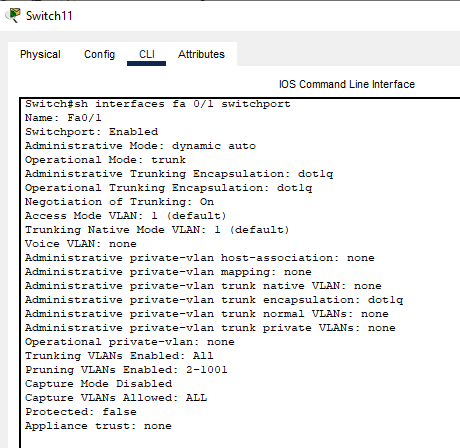
Отправка DTP-пакета устройству злоумышленника



Отправка DTP-пакета от устройства злоумышленника



В результате на коммутаторе устанавливается состояние порта trunk (operational mode) и через злоумышленника будет проходить весь трафик

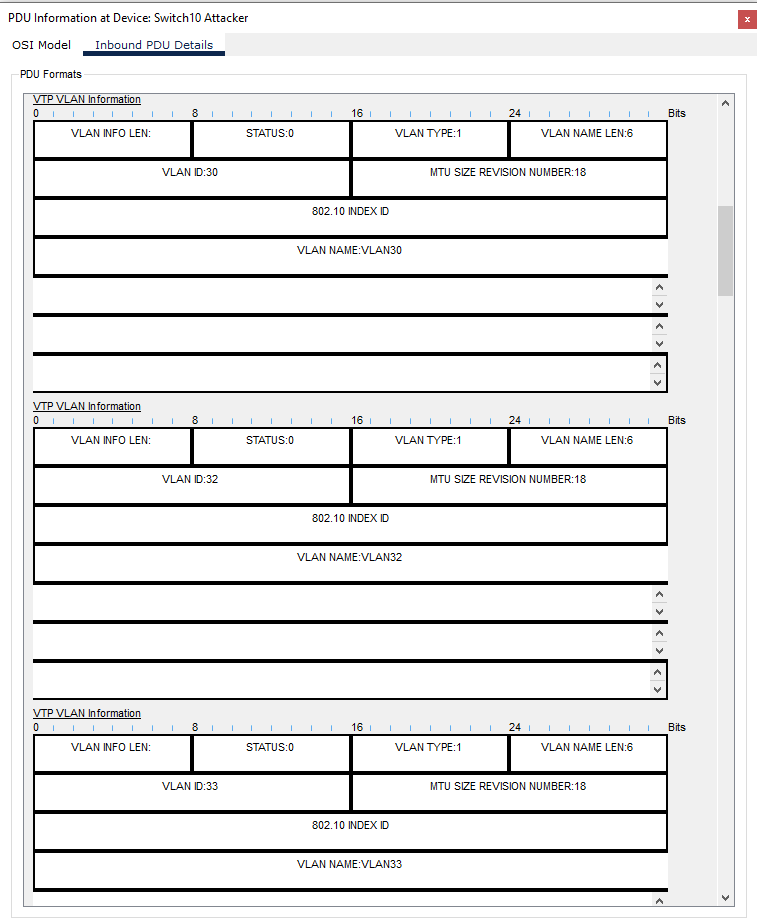


3. Уязвимость VTP

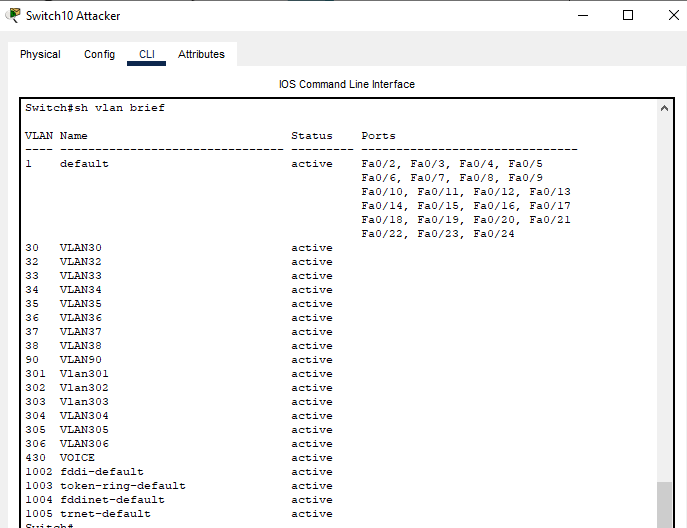
На attacker настраиваю

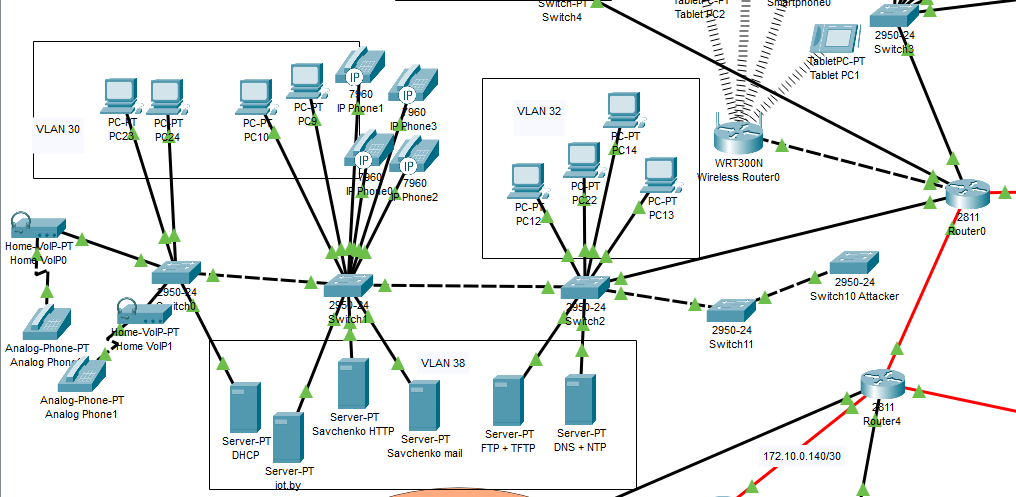






На рисунке – получение злоумышленником vtp

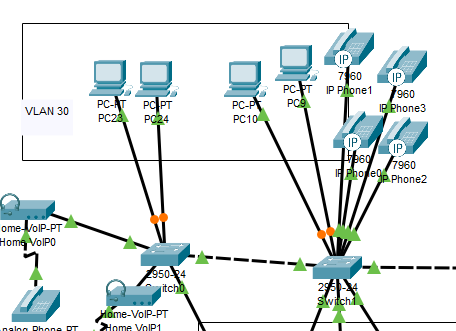




Далее реалтзую атаку, на свиче атакера прописывааю #no vlan 30

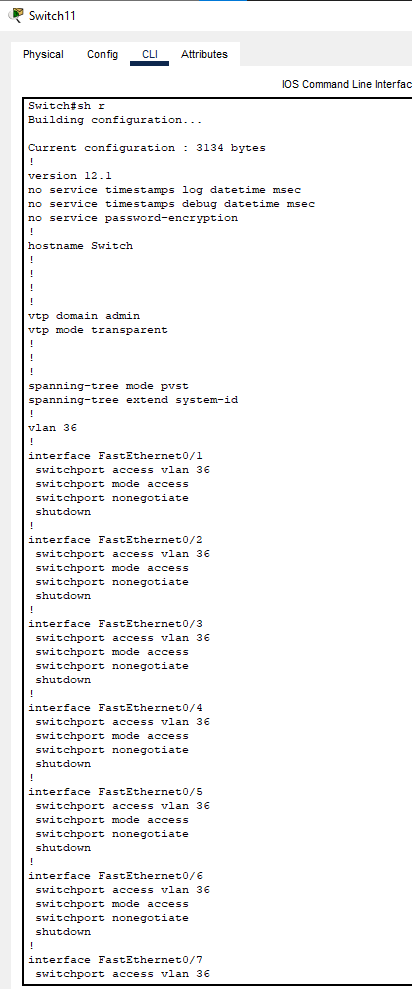


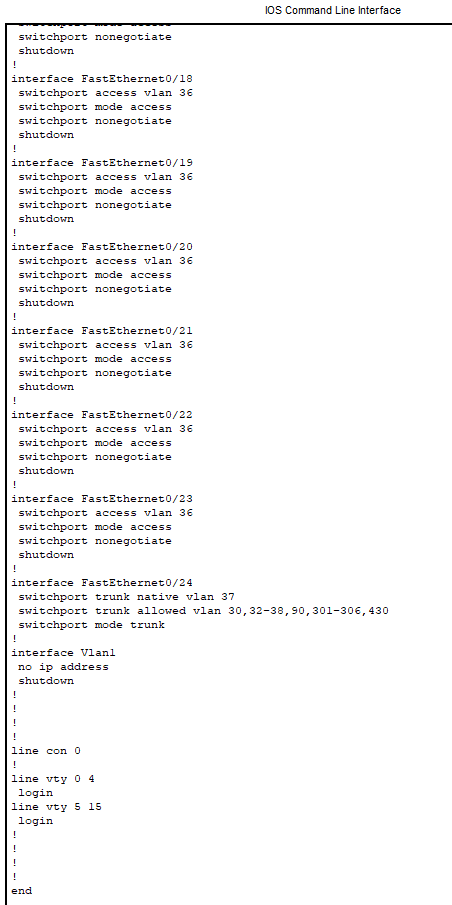
Примерно через 5 минут мой vlan 30 оказался «оторваным» от всей остальной сети



4.защита

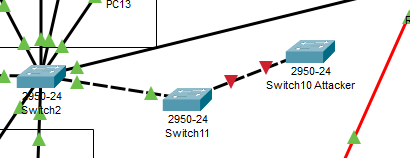
Пример конфигурации коммутатора switch 11



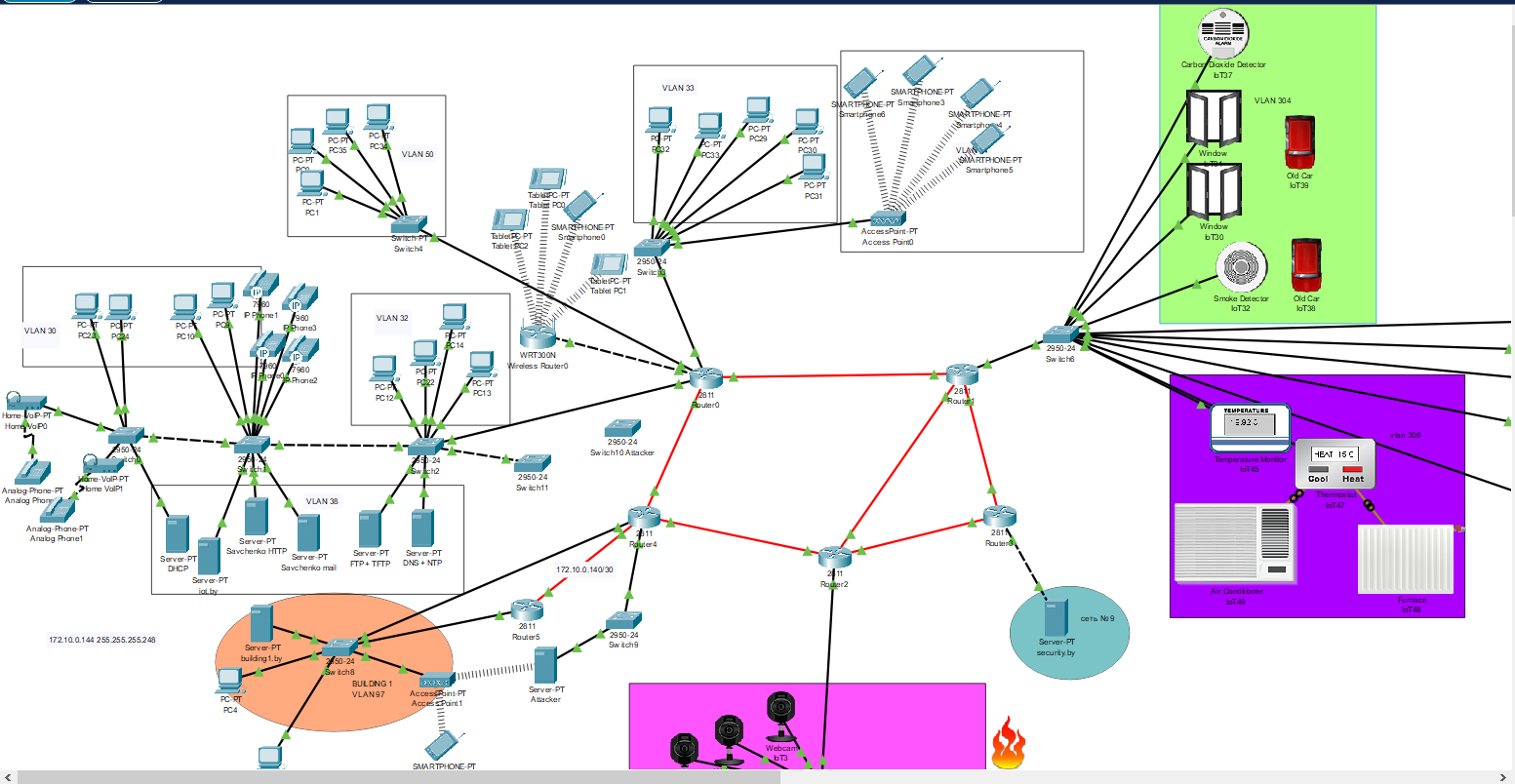


5. Попытка провести атаку

При попытке согласования портов и подключение к сети у злоумышленника ничего не вышло



**Вывод:** помимо больших преимуществ использования VLAN, они имеют и свои минусы, которые я рассмотрела в данной лабораторной работе. Vlan-hooping основан на том, что коммутаторы умеют автоматически согласовывать порты с помощью DTP-протокола, что являлось первой уязвимостью, благодаря ей, злоумышленник легко присоединился в сеть и дальше мог использовать уязвимость протокола VTP, то есть узнать какте VLAN есть в сети и дальше оповестить всем ложную информацию, допустим о том что такого влана больше не существуют, и все остальные коммутторы удаляют его из своей базы, а устройства удаленного влана больше не могу получить ни к чему доступ. Чтобы такого не происходило были рассмотрены и реализованы принципы защиты, после всех настроек было проверено, что больше злоумышленник не может подключиться в сеть и совершать никаких злых действий.

****